Cisco Process Orchestrator Hardening Guide

Introduction

Securing your Cisco Process Orchestrator installation requires adjustments at various levels of you infrastructure. From your Windows® servers to the applications and resources used by Process Orchestrator this guide will discuss the various points of vulnerability in Process Orchestrator and explain the best practices that can be employed to make your installation more secure.

Note: Complying with these hardening guidelines does not guarantee the elimination of all security threats. However, by implementing these guidelines, you can achieve a higher-level of security and help manage unforeseen risks.

Recommended Windows Security Hardening Policy

This section describes the steps required to allow a hardened windows system using Microsoft Windows recommended hardening guidelines to properly run Process Orchestrator, as well as to make additional changes to harden its configuration. If your system has additional hardening steps, further changes may be required to get Process Orchestrator to work.
For hardening Windows Server 2008 R2 and 2012, the Best Practices Analyzer (BPA) server management tool, which is installed by default on all editions of Windows Server 2008 R2 and Windows Server 2012, except the Server Core installation option, can be used.
This server management tool helps administrators reduce best practice violations by scanning one or more roles that are installed on your Windows Server and reporting best practice violations to the administrator.
For additional information on recommended Windows OS hardening guidelines, see Microsoft Security Compliance Manager.

Recommended Microsoft SQL Server Hardening Best Practice

Applications that are not included with Windows Server 2008 R2 have a separate Best Practice Analyzer (BPA) for optimizing and hardening applications. These BPAs run on an application called the Microsoft Baseline Configuration Analyzer (MBCA) which help maintain optimal system configuration by analyzing configurations of a company's computers against a predefined set of best practices.
To download MBCA v2.0, click http://www.microsoft.com/download/en/details.aspx?id=16475.

The Microsoft SQL Server 2008 R2 BPA is a diagnostic tool that gathers information about a server and a Microsoft SQL Server 2008 or 2008 R2 instance installed on that server and recommends solutions to potential problems.
To download the SQL Server 2008 R2 Best Practices Analyzer, click http://www.microsoft.com/download/en/details.aspx?id=15289. Similarly, there is a tool for SQL Server 2012. To download the SQL Server 2012 Best Practices Analyzer, click http://www.microsoft.com/en-us/download/details.aspx?id=29302.

Recommended Steps for Hardening Oracle Database

For information on hardening an Oracle 11g or 12c database please refer to the **Oracle Database Hardening Guide.**

Ports Used By Process Orchestrator Server[1]

Process Orchestrator utilizes various TCP ports to facilitate communication between the server and its different clients. By default an Orchestrator server will open a port for use by the Orchestrator Console (see **Error! Reference source not found.**).

Default Port	Use
61525	Orchestrator Console
61526	Secure Web Service
61527	Non-secure Web Service

Table 1 - Default Port Assignments

You can see which ports are in use by any given Orchestrator server through the Orchestrator Console. Go to the Administration view and select Orchestrator Servers as seen in the screenshot below:

[1] Refer to the Cisco Process Orchestrator Port and Services section of the Installation Guide for additional information.

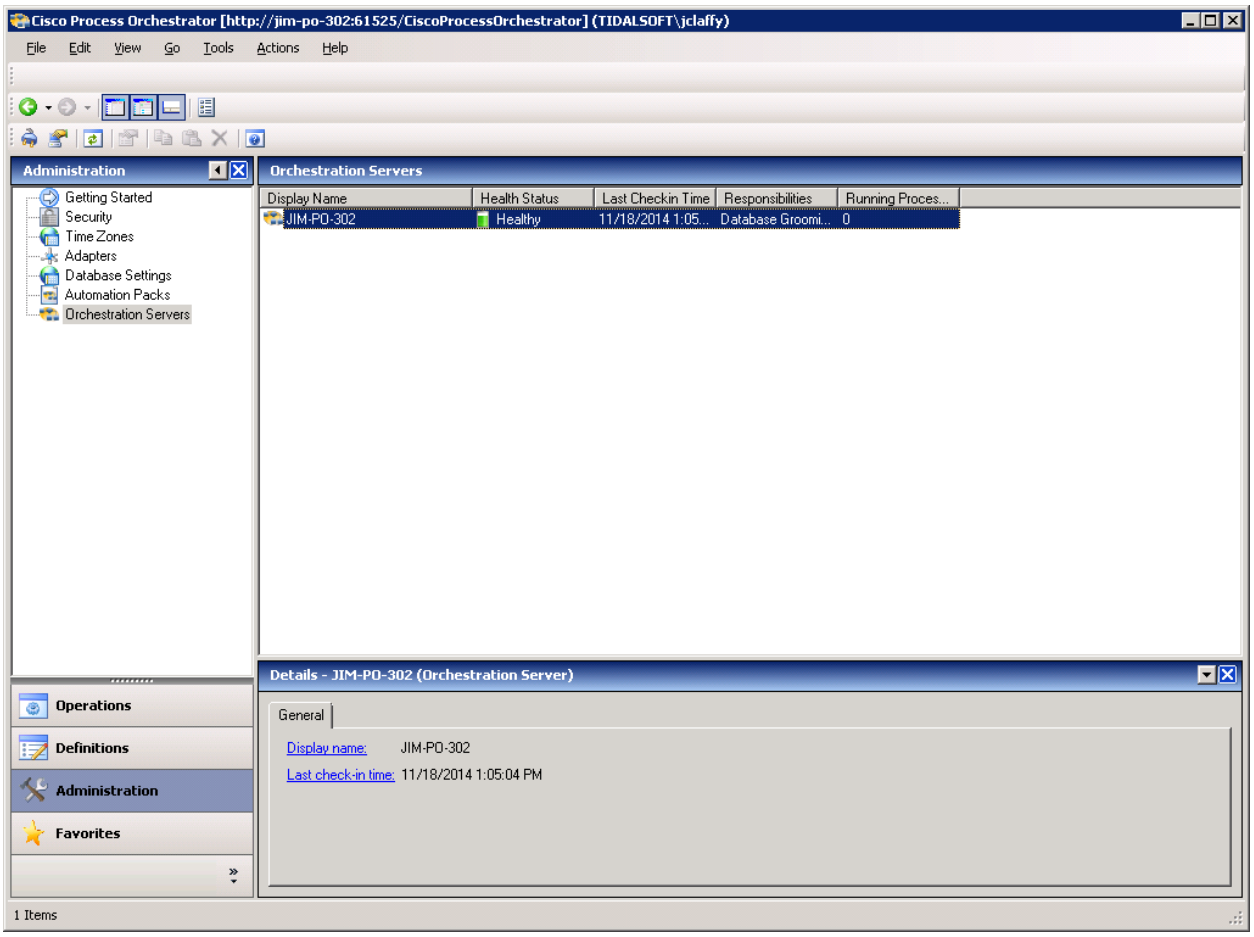

Figure 1 - Orchestrator Servers View

Double-clicking on a server and selecting the ports tab reveals the following dialog:

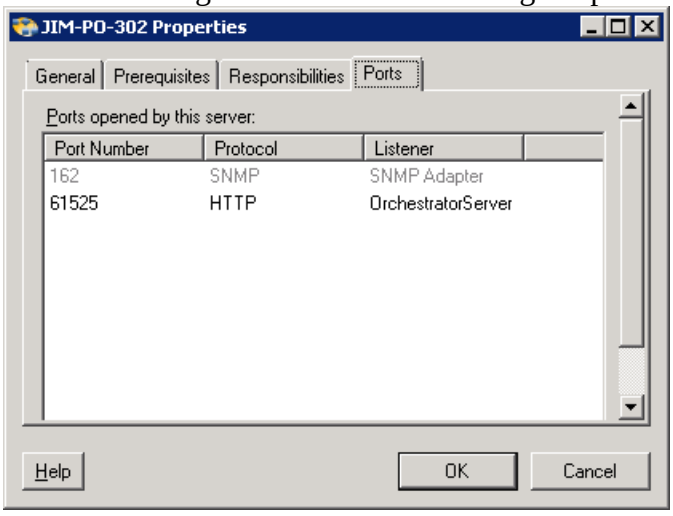

Figure 2 - Orchestration Server Properties

Changing Orchestrator Default Ports

Process Orchestrator Console Port

Step 1 Choose **Start > Control Panel > Administrative Tools > Services**.
The Services dialog box displays.

Step 2 Select **Cisco Process Orchestrator Server**, right-click and choose **Stop**.
Leave the Services dialog box open.

Step 3 In the Cisco Process Orchestrator install directory, open the following configuration files and modify the port number to a non-default port number.
The XML files open in the default application associated with the file. If the file does not open by default, then use *Notepad.exe* to open the file.

Configuration File Instructions

Tidal.Automation.Server.exe.config
Scroll to the *ClientCommunicationPort* and change the value to a non-default port, such as *11111*. Document the port number elsewhere for later use.

Tidal.Automation.Console.Loader.exe.config
Scroll to the *Server URL* and change port number to match the ClientCommunicationPort number in the *Tidal.Automation.Server.exe.config* file. Note: This file needs to be modified on the all machines where the Console is installed, including remote Consoles.

Web.config
Located in the WebConsole folder this file needs to be modified so that the WebServiceUris property contains the same port number as the one configured in *Tidal.Automation.Server.exe.config*.

Tidal.Automation.WinForms.AutomationPackManagement.Wizard.Setup.exe.config
This file exists in the Console folder under the Cisco Process Orchestrator install directory. Modify the URL "http://localhost:%NewPortNumber%" in this file with the new port number.

Tidal.Automation.CLI.CorePSSnapin.dll.config
Modify the URL "http://localhost:%NewPortNumber%" in this file with the new port number.

Step 5 Save and close each file after the port number is changed.

Step 6 Return to the Services dialog box and restart the Cisco Process Orchestrator Server service.

Northbound Web Service Ports

The Northbound Web Services offered by the Orchestrator server are available on both secure and unsecure ports (see **Error! Reference source not found.**). Securing the NBWS ports can take on two forms. Firstly, the port assignments can be changed from their default. Secondly, the security certificate assigned to the secure NBWS port can be changed from the default certificate generated by the Orchestrator server. Refer to the Cisco Process Orchestrator

Northbound Web Services Guide for instructions on changing the ports used by the server to listen for connections to its Northbound Web Services and for instructions on utilizing an alternate certificate for the secure NBWS port.

Ports Used by Orchestrator Adapters

In addition to the ports used by the Orchestrator server, the various adapters loaded by the server may either listen on additional ports or connect to ports on remote servers. In general, many adapters allow the user to specify port numbers when configuring targets (i.e. SNMP, Email, Service Catalog, VMware vSphere, JMX, etc.) and these ports need to be accounted for when configuring firewalls or other network security tools.

SNMP

When functioning as an SNMP manager the SNMP adapter will listen for traps on UDP port 162. The SNMP adapters *Trap listening port* can be changed through the SNMP Adapter configuration as seen in the screenshots below:

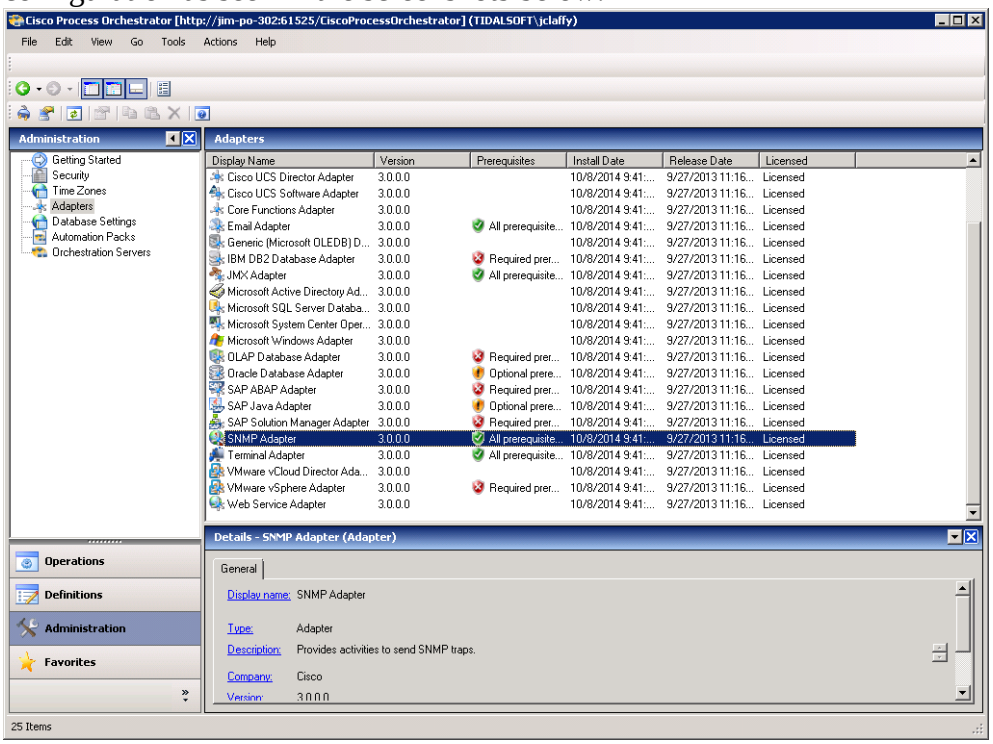

Figure 3 – Adapters

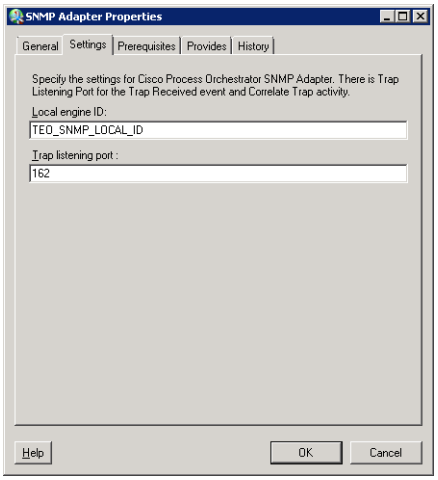

Figure 4 - SNMP Adapter Configuration

When functioning as an SNMP agent the SNMP adapter will send traps to an SNMP manager on port 162 by default. The port assignments can be changed via the SNMP target configuration as seen in the screenshots below:

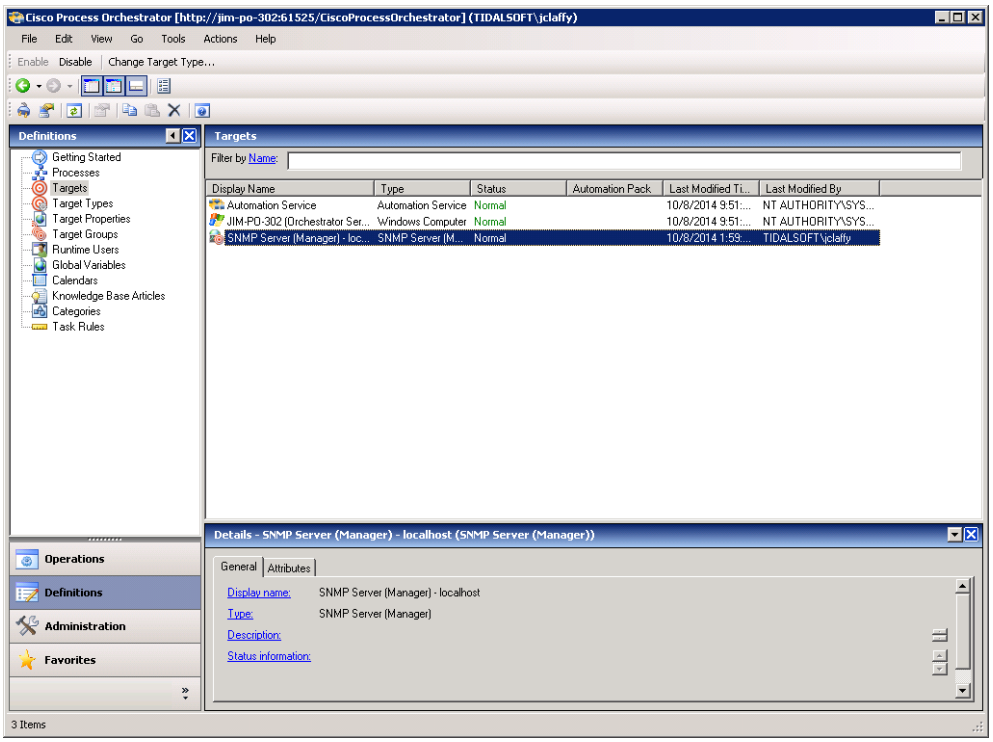

Figure 5 - Target Configuration

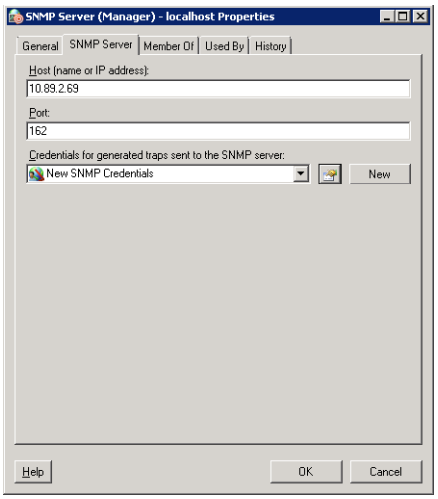

Figure 6 - SNMP Manager Target Configuration

When functioning as an SNMP manager the adapter will make requests (get, getnext, etc) to UDP port 161 of the SNMP agent by default. The port assignments can be changed via the SNMP target configuration as seen in the screenshots below:

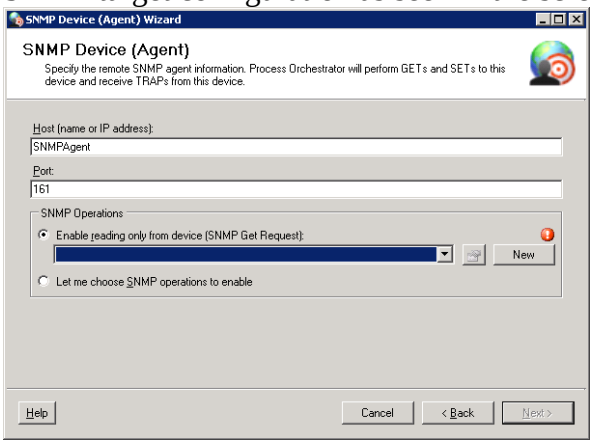

Figure 7 - SNMP Agent Target Configuration

Other Ports

One adapter of special note is the Windows adapter which makes use of various protocols which depend on certain ports being opened on remote servers. Activities in this adapter are using RPC calls to talk to remote machine. The ports required by RPC calls are controlled by the OS itself.

"Remote Procedure Call (RPC) dynamic port allocation is used by server applications and remote administration applications such as Dynamic Host Configuration Protocol (DHCP) Manager, Windows Internet Name Service (WINS) Manager, and so on. RPC dynamic port allocation will instruct the RPC program to use a particular random port in the range configured for TCP and UDP, based on the implementation of the operating system used (see references below).

Customers using firewalls may want to control which ports RPC is using so that their firewall router can be configured to forward only these Transmission Control Protocol (UDP and TCP) ports."

For more information see http://support.microsoft.com/kb/154596

Cisco Process Orchestrator Hardening Guide